


<p>Havells India Limited Havells India Physical Security Management Policy Version 1.0 Internal</p>	 HAVELLS
---	---

Havells India

Physical Security Management Policy

Version 1.0

Havells India Limited Havells India Physical Security Management Policy Version 1.0 Internal	 HAVELLS
---	---

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Havells India Physical Security Management Policy
2.	Document Code	HPSMP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Havells India Limited Havells India Physical Security Management Policy Version 1.0 Internal	 HAVELLS
---	---

Document Scope

This document shall be applicable to all employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose5

1.1 Scope5

1.2 Responsibility5

1.3 Enforcement5

1.4 Authority5

2. Policy6

2.1 Physical Security Perimeter6

2.2 Physical Entry Control6

2.3 Protecting against external and environmental threats9

2.4 Equipment Security 10

2.5 Contact with Authorities 12

<p>Havells India Limited</p> <p>Havells India Physical Security Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	
--	---

1. Purpose

This policy defines appropriate security controls required to protect information assets and information processing facilities of Havells from unauthorized use, access, and environmental threats.

1.1 Scope

This policy shall be applicable to the all employees/Third Party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the Local Admin and concerned IT Team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the Physical Security Management Policy.

1.3 Enforcement

All Employees and/or Third Party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

- a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.
- b) Employees and Third Parties who breach this policy shall be subject to disciplinary action.

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy*.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

<p style="text-align: center;">Havells India Limited Havells India Physical Security Management Policy Version 1.0 Internal</p>	
--	---

2. Policy

2.1 Physical Security Perimeter

Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities. Physical protection shall be achieved by creating several physical barriers around the business premises and information processing facilities.

The following guidelines and controls shall be considered and implemented where appropriate:

- a) The security perimeter shall be clearly defined;
- b) The perimeter of a building or site containing information processing facilities shall be physically sound. The external walls of the site shall be of solid construction and all external doors shall be suitably protected against unauthorized access, e.g., control mechanisms, alarms, locks etc.;
- c) A manned reception area or other means to control physical access to the building shall be in place. Access to building shall be restricted to authorized personnel only;
- d) Physical barriers shall, if necessary, be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding;
- e) All fire doors/exits on a security perimeter shall be monitored, and tested in conjunction with the walls to establish the required level of resistance;
- f) Information processing facilities managed by the organization shall be physically separated from those managed by third parties.

2.2 Physical Entry Control

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The following controls shall be implemented to ensure adequate protective measures:

- a) Each employee shall be allowed the access through Face Reader/Biometric access control machine.
- b) Visitors to secure areas shall be supervised, and their date and time of entry and departure recorded; and
- c) Access rights to secure areas shall be regularly reviewed and updated by management responsible for the specified areas, wherever required.

2.2.1 Securing facilities

The selection and design of a secure area shall be taken into account the possibility of damage from fire, flood, explosion, accident, malicious intent, and other forms of natural or man-made disaster. Consideration shall be given also to any security threats presented by neighbouring premises, e.g., leakage of water from other areas.

The following controls are essential considerations:

<p style="text-align: center;">Havells India Limited Havells India Physical Security Management Policy Version 1.0 Internal</p>	
--	---

- a) Doors and windows shall be locked when unattended and external protection shall be considered for windows, particularly at ground level;
- b) Hazardous or combustible materials shall be stored securely at a safe distance from a secure area;
- c) Fallback equipment and back-up media shall be sited at a safe distance to avoid damage from a disaster;
- d) Any outlying buildings or areas that house/contain data centre support equipment (backup generators, cooling towers, UPS, etc) shall have the similar level of security controls as the data centre itself; secure structure, access control, and technical surveillance systems for monitoring access and activities around the area. Surveillance and monitoring are subject to legal limitations in many jurisdictions, and shall be subject to contractual limitations in union, Works Council, or shop agreements. Legal Counsel shall be consulted before implementing these measures;
- e) A manned reception area or other means to control physical access to the building shall be in place. Access to the building shall be restricted to authorized personnel only;
- f) Visitor control procedures shall be implemented to ensure that all visitors to the company facilities are positively identified and authorized prior to granting access to facility. Visitors register is maintained to record purpose, date, and time of visit. Visitors shall only be granted access for specific, authorized purposes. Visitor control Logs shall be established and maintained;
- g) Wherever possible, Technical Surveillance Systems (CCTV) shall be utilized to monitor activities around the immediate environs of the building and entrances. This surveillance shall be discussed with security team prior to use;
- h) All safety/fire emergency doors shall be alarmed and have closing and locking mechanisms.

2.2.2 CCTV

- a) All new camera systems and/or replacement systems shall be approved by the Admin Head and recorded in register of CCTV cameras;
- b) The recording devices/servers for CCTV cameras shall be installed in a secure location as approved by the Admin Head. Only personnel trained and authorized as CCTV Operators shall be allowed access to recorded CCTV footage;
- c) All footage shall be kept for the maximum of 15 days depending upon hardware and storage capacity;
- d) Live streaming camera monitoring shall be restricted to locations where it is necessary, depending on the purpose of the camera. For example, when the purpose of the camera is to monitor public activity around main reception area, the camera live feed may be viewed by designated Havells employees and contractors;
- e) Where cameras are monitored via a mobile device (such as a smartphone, tablet, or similar device), a CCTV Controller shall ensure that no unauthorized person has the ability to view the device;

Admin In charge	Full System Access to all CCTV camera features and Programming.	Admin In charge
CCTV Controller	Full System Access to all CCTV camera features and programming maintenance purposes.	Designated staff
CCTV Operator	Majority system access for all cameras on their site including Programming ability, live playback and export.	Managers and Supervisory Staff
CCTV View only	Live View, Playback (no export)	Designated Staff

- f) CCTV surveillance shall be carried out 24x7
- g) Recorded footage is confidential. All requests to view footage relating to individuals shall be referred to Admin Head and HOD for approval. A list of approved persons or entities shall be maintained in the CCTV Access Log;
- h) Individual cameras and/or camera areas shall have a sign posted to notify the public. Signs shall clearly display the message "You Are under CCTV Surveillance" or "24 Hour CCTV Surveillance in Operation" or a similar message and be of a size and style that makes them readily visible to people entering the area covered by CCTV Surveillance.

2.2.3 Working in secure areas

Any sensitive area shall be identified and located in a physically separate, secure area. Access to this area shall be monitored.

The following guidelines may be considered:

- a) Access to sensitive information and information processing facilities, shall be controlled and restricted to authorized persons only. Authentication controls, (e.g., Card/Biometric), shall be used to authorize and validate all access; and
- b) Access rights to secure areas shall be regularly reviewed.

2.2.4 Isolated Delivery Loading Areas

Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

The following controls shall be considered:

- a) Access to a holding area from outside of the building shall be restricted to identified and authorized personnel;
- b) The holding area shall be designed so that supplies can be unloaded, without delivery staff gaining access to other parts of the building;
- c) Incoming material shall be inspected for potential hazards and registered, if appropriate, before it is moved from the holding area to the point of use; and
- d) Incoming and outgoing shipments shall be physically segregated; wherever required.

<p>Havells India Limited</p> <p>Havells India Physical Security Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	
--	---

2.3 Protecting against external and environmental threats

All Havells information processing facilities shall adhere to this policy, for the implementation of controls to protect the information assets and facilities hosting information against damage from external and environmental threats like fire, flood, earthquake, explosion, civil unrest and other forms of natural and manmade disaster.

- a) Protection measures shall be implemented considering the potential events such as flood, earthquake, explosion, civil unrest etc.;
- b) The site building shall suffice the minimum seismic tolerance capability as per the seismic zone applicability;
- c) The server and utilities room shall not be located on the top floor or basement of the site building or in any such area where proper entry or exit are not provisioned;
- d) The floor and ceiling of the building shall be constructed of non-combustible or limited combustible materials.

2.3.1 Fire Safety

License / Clearance from Local Administrative Authorities / Law Enforcement Agencies if required as per law shall be obtained and maintained for fire safety measures implemented and any other such requirement emerging from time to time.

2.3.2 Fire Prevention

- a) Combustible material shall not be stored in the proximity of electrical panels, distribution boxes, lighting equipment etc.;
- b) Cable ducts or other penetrations in the server rooms shall be fire stopped with a listed fire stopping material that has a fire rating equal to the fire-resistance rating of the penetrated barrier;
- c) Smoking shall not be allowed within the facility.

2.3.3 Fire Detection and Warning System

- a) Appropriate fire protection measures, including installation of fire detection and suppression systems shall be implemented;
- b) All locations in the building shall have fire/ smoke detection system of requisite type and capacity installed;
- c) Fire detection and alarm system, emergency lighting system shall have independent UPS of required capacity and shall also have an alternate power source available;
- d) There shall be a suitable Public Address (PA) mechanism (PA system) that shall cover each floor and every part of the building. All personnel working in the building shall be able to clearly hear any warnings/ announcements being made on the PA mechanism irrespective of the area within the premises they are working;

<p style="text-align: center;">Havells India Limited Havells India Physical Security Management Policy Version 1.0 Internal</p>	
--	---

- e) Fire alarm system shall be installed on each floor of the building; and
- f) There shall be one integrated fire monitoring area in building and fire detection control / Fire suppression / equipment shall be present in the entire facility.

2.3.4 Emergency Response Plan and Evacuation Drills

- a) Creation and implementation of emergency evacuation plans including the formation of an Emergency Response Team (ERT) hosting Havells information assets to ensure emergency evacuation;
- b) The building shall have adequate fire exits and stairways;
- c) Evacuation drills shall be carried out once in every six months at Havells office;
- d) The security guards shall be trained in the manual rescue in case of any emergency;
- e) All emergency numbers shall be displayed on floors/ vulnerable areas;
- f) Fire/floor wardens shall be identified and adequately equipped and trained to handle fire incidents;
- g) Site evacuation map shall be displayed at prominent locations of each floor. Safety norms on fire evacuation shall be displayed at prominent areas;
- h) Safe assembly point shall be identified, labelled, and displayed prominently;
- i) Fire/floor marshals shall be equipped for communication; and
- j) First aid kits shall be made available and placed at the reception.

2.4 Equipment Security

Adequate controls shall be designed and implemented for equipment security to prevent loss, damage, theft, or compromise of information systems processing Havells' information and to prevent interruption to Havells' activities.

2.4.1 Equipment Location and Protection

All equipment shall be protected against environmental threats and unauthorized access. IT team shall ensure that:

- a) The equipment is appropriately located, and adequate security controls are implemented for their continued operations;
- b) Unattended equipment such as servers, network, wireless and electrical devices are placed in secure enclosures and locked;
- c) Raised floor at server shall be of non-combustible material and shall incorporate provisions for drainage from domestic water leakage, sprinkler operation at other places, coolant leakage etc.;
- d) The server rooms shall be physically separated from the UPS/ Battery room; and
- e) Appropriate controls shall be designed and implemented to protect the equipment from environmental hazards.

2.4.2 Supporting Utilities

All equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

2.4.2.1 Generator and Fuel Storage

- a) The Diesel Generator (DG) system (N + 1) capacity shall be sized to take the entire building load;
- b) The fuel storage tank shall have industrial grade overhead shade;
- c) No vehicular parking and storage shall be allowed in the fuel storage tank area;
- d) The on-site fuel storage shall be sized to cater minimum of generator operations 72 hours;
- e) License / Clearance from Local Administrative Authorities / Law Enforcement Agencies shall be obtained and maintained for fuel storage and any other such requirement emerging from time to time; and
- f) Over current, over voltage, under voltage, reverse power, over speed, high temperature, Low fuel level shall be alarm monitored.

2.4.2.2 UPS System

- a) UPS system installed at the site shall be with a minimum 15-minute battery back-up time on full load;
- b) Dual power source shall be available at UPS input panel;
- c) Battery current & voltage shall be monitored and recorded. Battery Discharge check shall be performed once in a year.

2.4.2.3 HVAC System

HVAC system shall be installed and following controls shall be implemented

- a) The temperature and humidity shall be controlled to provide continuous operating ranges for temperature and humidity:
 - i. Temperature: 22°C +/- 2°C;
 - ii. Relative Humidity: 40% to 55%;
- b) The redundant power source to HVAC system shall be maintained;
- c) Tower split AC shall be maintained with n+n redundancy; and
- d) The UPS room & electrical room shall have redundant continuous rated industrial ACs in place to adequately maintain the temperature at desired condition.

2.4.3 Cabling Security

Appropriate controls shall be designed and implemented to protect power and cables carrying data or supporting information services, from unauthorized interception or damage. It shall be ensured that:

- a) All cables and their corresponding terminals are identified and marked appropriately;

<p>Havells India Limited</p> <p>Havells India Physical Security Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	
--	---

- b) Loose terminations, unused openings shall not exist in any of the electrical power distribution boards;
- c) Water pipes shall not be placed over or adjacent to any electrical ducts; and
- d) Power cables are segregated from communication cables to prevent interference.

2.4.4 Equipment Maintenance

- a) All equipment shall be properly maintained to ensure their continued availability and integrity for proper uninterrupted business activities;
- b) All supporting utilities, such as electricity, water supply, sewage, heating/ventilation and air conditioning, diesel generator, UPS, battery bank, transformer, fire detection and suppression systems, electrical panels are in appropriate condition for the information systems and/ or facilities that they are supporting. They shall be maintained and AMCs with approved vendors shall be used;
- c) IT team shall ensure that preventive maintenance for all IT devices is carried out at regular intervals for continuous availability of these systems;
- d) Maintenance of equipment shall be carried out as per the manufacturer's instructions and specifications;
- e) Routine maintenance and repair shall be carried out by authorized maintenance personnel only; and
- f) All equipment's OEM manual/SOP shall be maintained & updated.

2.4.5 Secure Disposal and Re-use of Equipment

- a) The process for accounting of removed storage media, storing it securely till degaussed, and then following a secure process for disposing the degaussed storage media shall be implemented;
- b) All information / data and licensed software shall be removed or securely over-written prior to the disposal of any equipment containing storage media;
- c) Destruction/disposal of media shall be done securely in accordance with approved tools and methods;
- d) Equipment containing or having contained information assets of Havells shall be disposed of only after obtaining approval from authorized personnel; and
- e) If required, before sending any equipment out for repair, it shall be securely wiped to ensure that it does not contain any sensitive data;

2.4.6 Removal/Discard of Assets

All employees shall ensure that any equipment, information, information systems, storage devices and/or software of Havells are discarded or removed as per Capex SOP and as per applicable statutory provisions.

2.5 Contact with Authorities

Havells India Limited Havells India Physical Security Management Policy Version 1.0 Internal	 HAVELLS
---	---

Havells shall maintain contact with authorities including but not limited to law enforcement authorities, regulators, fire department, and emergency services. The contact details of these agencies shall be maintained and displayed at prominent places.